Homeland Security

Daily Open Source Infrastructure Report
08 July 2015

Top Stories

- The U.S. Securities and Exchange Commission charged San Francisco-based Luca International Group and its chief executive officer with running a $68 million Ponzi-like scheme targeting Chinese-American investors, July 6. – *U.S. Securities and Exchange Commission* (See item **4**)

- The Huntsville Madison County 9-1-1 Center reported July 7 that its main phone system and back-up system were down July 4 after a car wreck severed power lines. – *WAAY 31 Huntsville* (See item **12**)

- Iowa City officials reported July 6 that a convicted armed robber escaped from the Iowa State Penitentiary in Fort Madison after climbing to the roof and using a makeshift rope to reach the ground. – *Associated Press* (See item **14**)

- A 4-alarm fire at an Upper Darby, Pennsylvania Payless Shoe Store prompted the evacuation of several businesses and about 200 first responders to contain the incident. – *WPVI 6 Philadelphia* (See item **20**)

Fast Jump Menu

Energy Sector

1. *July 6, San Francisco Chronicle* – (California) **Report on Fresno gas explosion cites pipe's reduced dirt cover.** The California Public Utilities Commission released a report July 6 revealing that an April 17 Pacific Gas and Electric gas pipeline explosion, caused when an earthmoving truck struck the pipeline was a result of inadequate depth of cover and failure by the company to properly mark its presence.
Source: http://www.sfgate.com/news/article/Report-on-Fresno-gas-explosion-cites-pipe-s-6369645.php

2. *July 6, Arlington Heights Daily Herald* – (Illinois) **Aurora homes evacuated due to gas leak.** Fourteen homes and one business in Aurora, Illinois were evacuated July 6 after a construction crew ruptured a four-inch gas main on North Spencer Street. Surrounding streets were closed for about six hours as crews worked to cap the leak.
Source: http://www.dailyherald.com/article/20150706/news/150709412/

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

For another story, see item **15**

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

3. *July 7, Help Net Security* – (International) **Hackers targeting users of Barclays, Royal Bank of Scotland, HSBC, Lloyds Bank and Santander.** Security researchers from Bitdefender warned of a malicious phishing scheme targeting financial users of banks worldwide, including Bank of America, Citibank, Wells Fargo, JP Morgan Chase, and PayPal in the U.S., in which spam servers are distributing emails directing users to download an archive containing a downloader for the Dyreza banking trojan. The three-day campaign has so far distributed 19,000 emails worldwide.
Source: http://www.net-security.org/malware_news.php?id=3070

4. *July 6, U.S. Securities and Exchange Commission* – (International) **SEC charges oil company and CEO in scheme targeting Chinese-Americans and EB-5 investors.** The U.S. Securities and Exchange Commission charged San Francisco-based Luca International Group July 6 and its chief executive officer with running a $68 million

Ponzi-like scheme in which the company allegedly falsely portrayed itself to targeted Chinese-American investors in California as well as Chinese citizens through the EB-5 Immigrant Investor Program, and diverted investor funds to personal uses and profit repayments.
Source: http://www.sec.gov/news/pressrelease/2015-141.html

Transportation Systems Sector

5. *July 7, WSMV 4 Nashville* – (Tennessee) **Crews upright train cars after Berry Hill derailment; tracks expected to reopen this morning.** Tracks reopened July 7 after Crews righted four cars of a CSX train that derailed and overturned in Berry Hill, Tennessee July 6. Three of the cars were carrying polypropylene beads used for packaging, and no spills or injuries were reported.
Source: http://www.wsmv.com/story/29486568/officials-at-least-3-rail-cars-flipped-in-south-nashville

6. *July 7, KXAS 5 Dallas-Fort Worth* – (Texas) **Fatal crash involving motorcycle, 18-wheelers shuts down Interstate 30.** Authorities closed eastbound Interstate 30 in Dallas for approximately 4 hours while crews cleared the scene of a 2-vehicle wreck that involved a semi-truck and a motorcycle that killed 1 person, July 7.
Source: http://www.nbcdfw.com/news/local/Fatal-Wreck-Motorcycle-18-Wheelers-Shuts-Down-I-30-312000471.html

7. *July 6, KNTV 11 San Jose* – (California) **SF-bound Southwest flight from Arizona makes emergency landing in Phoenix.** San Francisco-bound Southwest flight from Phoenix returned to Sky Harbor Airport in Arizona shortly after take-off for an emergency landing due to a blown tire on the main landing gear July 6. The flight landed safely and no injuries were reported.
Source: http://www.nbcbayarea.com/news/local/SF-Bound-Southwest-Flight-from-Arizona-Makes-Emergency-Landing-in-Phoenix-311944541.html

8. *July 6, Kansas City Star* – (Missouri) **I-35 reopens five hours after gas link break near Liberty.** A stretch of Interstate 35 in Clay County reopened July 6 after being closed for more than 4 hours while crews repaired a gas line break in Pleasant Valley that spewed gas into the air next to the interstate, but did not cut off gas service to customers.
Source: http://www.kansascity.com/news/local/article26573548.html

Food and Agriculture Sector

9. *July 6, U.S. Department of Agriculture* – (National) **Lombardi Brothers Meats recalls steak and ground products due to possible E. coli O157:H7 contamination.** Lombardi Brothers Meat, a Denver, Colorado establishment, is recalling approximately 26,975 pounds of tenderized steak and ground beef products that may be contaminated with E. coli O157:H7. The items were produced from June 12 – June 30 and shipped to hotels, restaurants, and institutes nationwide.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-

alerts/recall-case-archive/archive/2015/recall-097-2015-release

For another story, see item **10**

Water and Wastewater Systems Sector

10. *July 6, Associated Press* – (Tennessee) **Toxic East Tennessee train derailment may have affected water.** Officials issued an activity advisory for Culton Creek in Tennessee after biologists found dead fish from the July 2 CSX train derailment that spilled toxic chemicals. Sample testing showed Pistol Creek and Little River were safe for normal activity while other cleanup efforts continue.
Source: http://www.timesfreepress.com/news/local/story/2015/jul/06/toxic-csx-derailment-may-have-dumped-chemicals-culton-creek/313164/

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

11. *July 6, WMDT 47 Salisbury* – (Maryland) **All clear given after bomb threat at UMES.** Approximately 150 construction workers and faculty members were evacuated from the University of Maryland Eastern Shore July 6 after a bomb threat was made to a construction site on the east side of campus. Students attending a summer program were dismissed early.
Source: http://www.wmdt.com/news/more-local-news/officials-investigating-bomb-threat-at-umes/34012858

Emergency Services Sector

12. *July 7, WAAY 31 Huntsville* – (Alabama) **9-1-1 center phone system fails again.** The Huntsville Madison County 9-1-1 Center reported July 7 that its main phone system and back-up system were down July 4, after a car wreck severed power lines and an uninterruptible power source malfunctioned. Officials are working to resolve future outages.
Source: http://www.waaytv.com/appnews/center-phone-system-fails-again/article_ec0592a0-2411-11e5-8ca1-efcb395ebdfb.html

13. *July 6, WABC 7 New York* – (New Jersey) **Car chase involving stolen police cruiser sweeps through 7 New Jersey towns.** The Englewood Cliffs Police Department arrested a Connecticut man July 6 after he stole a civilian vehicle and a police cruiser, leading several officers to pursue the suspect in an extended car-chase. Five officers were injured and sent to area hospitals for non-life threating injuries.
Source: http://7online.com/news/stolen-police-cruiser-chase-sweeps-through-7-new-jersey-towns/830186/

14. *July 6, Associated Press* – (Iowa) **Inmate escapes maximum-security prison through**

pipes. Iowa City officials reported July 6 that a convicted armed robber escaped from the Iowa State Penitentiary in Fort Madison after climbing to the roof through the facilities' piping, and used a makeshift rope to reach the ground. The prisoner was captured several hours later, about 100 miles from the prison.
Source: http://nypost.com/2015/07/06/inmate-escapes-maximum-security-prison-through-pipes/

For another story, see item **20**

Information Technology Sector

15. *July 7, Help Net Security* – (International) **Flaw allows hijacking of professional surveillance AirLive cameras.** Engineers from Core Security discovered vulnerabilities in AirLive's surveillance cameras in which an attacker could invoke computer-generated imagery (CGI) files without authentication or utilize backdoor accounts to execute arbitrary operating system commands, possibly allowing the attacker to see camera's transmission stream and compromise network devices.
Source: http://www.net-security.org/secworld.php?id=18597

16. *July 6, Threatpost* – (International) **Fraudulent BatteryBot Pro app yanked from Google Play.** Google pulled a malicious spoof of the Android BatteryBot Pro app from its Play service after Zscaler researchers discovered that the app requested excessive permissions from users in an attempt to gain full control of affected devices, supposedly to download and install other malicious Android packages and profit from click fraud, ad fraud, and SMS fraud. Once the app is granted admin privileges, it is impossible to uninstall.
Source: http://threatpost.com/fraudulent-batterybot-pro-app-yanked-from-google-play/113630

17. *July 6, Help Net Security* – (International) **Old MS Office feature can be exploited to deliver, execute malware.** A researcher reported a vulnerability in Microsoft Office in which its Object Linking and Embedding (OLE) Packager could be leveraged to deliver malicious executable files embedded in Office documents without triggering security software.
Source: http://www.net-security.org/secworld.php?id=18596

For another story, see item **3**

Communications Sector

Commercial Facilities Sector

18. *July 7, WBMA-LD 58 Birmingham* – (Alabama) **Flames destroy auto shop, businesses in six-alarm Walker County fire.** A 6-alarm fire destroyed an auto shop and surrounding business in Walker County, Alabama after beginning at Big Guys Tires and spreading to other retail stores. No injuries were reported and an investigation is ongoing to determine the cause.
Source: http://www.abc3340.com/story/29488863/flames-destroy-auto-shop-businesses-in-six-alarm-walker-county-fire

19. *July 7, USA Today* – (Kentucky) **Fire ravages Louisville's famed Whiskey Row.** A 3-alarm fire destroyed three buildings located in Louisville's historic Whiskey Row July 6 after starting in one of the business' basements. No injuries were reported and total damages are unknown.
Source: http://www.usatoday.com/story/news/nation/2015/07/07/fire-ravages-louisvilles-famed-whiskey-row-buildings/29802589/

20. *July 7, WPVI 6 Philadelphia* – (Pennsylvania) **Homes, businesses evacuated due to 4-alarm Upper Darby fire.** Surrounding homes and businesses were evacuated July 6 after a 4-alarm fire began at a Payless Shoe Store in Upper Darby, Pennsylvania, prompting 200 firefighters and emergency workers to respond to the incident. The cause of the incident is under investigation.
Source: http://6abc.com/news/homes-businesses-evacuated-due-to-4-alarm-upper-darby-fire/831984/

Dams Sector

Nothing to report

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions: Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS
                                        Daily Report Team at (703) 942-8590

Subscribe to the Distribution List: Visit the DHS Daily Open Source Infrastructure Report and follow
                                        instructions to Get e-mail updates when this information changes.

Removal from Distribution List: Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.